GHIDUL UTILIZATORULUI DE INTERNET

PRIN PROGRAMELE NOASTRE DE EDUCAȚIE SI INSTRUIRE CIBERNETICĂ VĂ ASIGURĂM SIGURANȚA ÎN MEDIUL ONLINE!

CYBER AID
EDUCATIE CIBERNETICA

WinTech consulting

ProDefence
Cyber Security Services

CYSCOE
CLUSTERUL DE EXCELENȚĂ
ÎN SECURITATE CIBERNETICĂ

MEDIUL ONLINE - INTERNETUL

Accesul la mediul online aduce de la sine o serie de reguli scrise (sau nescrise) în legătură cu comportamentul utilizatorilor unul față de celălalt, dar și asupra conținutului publicat.

Interacțiunea dintre utilizatori

- Respectați ceilalți utilizatori;
- Evitați conflictele și instigările;
- Evitați comportamentului imoral sau indecent;
- Evitați comportamentul deliberat sau neglijent, care pune în pericol siguranța personală, sau a celorlalți utilizatori.

Conținutul mediului online

- Protejați-vă confidențialitatea online; deasemenea protejați confidențialitatea celorlalți atunci când vi se cere;
- Respectați drepturile de autor, fără excepții;
- Evitați falsificarea intenționată a informațiilor;
- Evitați reproducerea neautorizată a informațiilor.

MEDIUL ONLINE - INTERNETUL

Beneficiile utilizării Internetului sunt numeroase.
Ne conectează la o rețea nelimitată de informații și ne ajută în interacțiunea cu semenii noștri, indiferent de locația acestora, fiindu-ne necesare doar două dispozitive și o conexiune la Internet.

Prezența pe internet ascunde însă o serie de pericole care vă pot afecta atât viața privată, cât și pe cea profesională.

Pierderile datorate unui atac cibernetic pot fi:

- Date și informații personale
- Informații confidențiale/ secrete profesionale
- Financiare și bunuri
- Integritate personală/ profesională
- ... Vieți omenești

Combaterea atacurilor cibernetice se face prin:

1. Conștientizare
2. Educație
3. Protecție
4. Îmbunătățire continuă

1. **Conștientizare**
   - Înțelegerea și acceptarea pericolelor mediului online
   - Calcularea riscurilor la care suntem expuși
   - Calcularea pierderilor în caz de atac cibernetic
2. **Protecție**
   - Instalarea unei aplicații de protecție (antivirus)
   - Schimbarea parolelor cu unele mai complicate
   - Folosirea autentificărilor multiple (MFA / 2FA)
3. **Educație**
   - Parcurgerea unui curs de bază în educație cibernetică
   - Căutarea de informații despre protecție cibernetică
   - Parcurgerea unui curs specializat în educație cibernetică
4. **Îmbunătățire continuă**
   - Asumarea misiunii de a reduce decalajul competențelor de securitate cibernetică cu soluții care conectează învățarea continuă
   - Susținerea programelor de educație cibernetică

Foarte important!!!

Nu vă panicați dacă sunteți victima unui atac cibernetic! Cereți ajutor imediat, sau raportați autorităților competente!

1 Conștientizare

Care este rolul conștientizării atunci când vorbim despre aspecte ale securității cibernetice?

1.1 Conștientizarea asupra securității cibernetice este reprezentată de cunoștințele și mentalitatea pe care le dețin utilizatorii de resurse informatice pentru a se proteja pe ei înșiși, pe cei din jurul lor, precum și activele fizice și informaționale ale companiei.

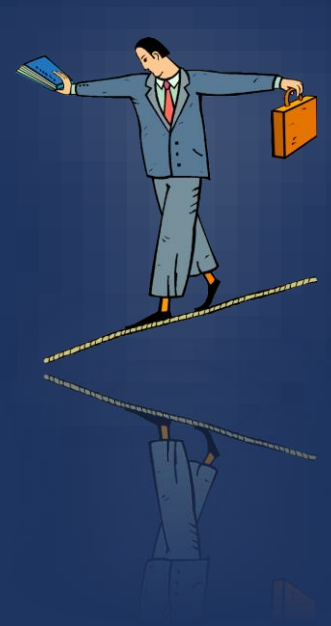
A fi „conștient” înseamnă:

- să înțelegeți că există posibilitatea ca unii oameni să provoace (în mod deliberat sau accidental) pierderi sau vătămări dumneavoastră, colegilor dumneavoastră sau activelor organizaționale;
- să înțelegeți riscurile la care sunteti expuși în online;
- să înțelegeți pierderile în caz de atac cibernetic.

1 Conștientizare

Care este rolul conștientizării atunci când vorbim de aspecte ale securității cibernetice?

1.2 Securitatea cibernetică se referă la tehnologiile, procesele și practicile concepute pentru a proteja activele informaționale ale unei organizații (computere, rețele, aplicații și date) de accesul neautorizat.
Odată cu creșterea frecvenței și severității atacurilor cibernetice, există o nevoie semnificativă de îmbunătățire a gestionării riscurilor de securitate cibernetică.



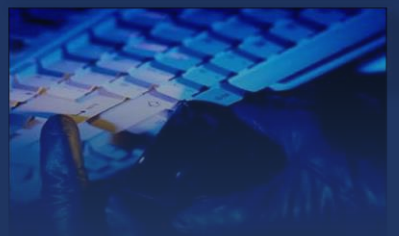
1 Conștientizare

Care este rolul conștientizării atunci când vorbim de aspecte ale securității cibernetice?

1.3 Securitatea datelor și sistemelor este crucială pentru toți. Informații despre tranzacții, fișiere personale, detalii despre contul bancar - toate aceste informații sunt adesea imposibil de înlocuit dacă sunt pierdute și ajung în mâinile infractorilor cibernetici.

Datele pierdute din cauza dezastrelor naturale (inundație, sau incendiu) sunt devastatoare, dar pierderea lor din cauza hackerilor sau a unei infecții cu malware poate avea consecințe mult mai grave.

Modul în care gestionați și protejați datele dvs. este esențial pentru securitatea afacerii dvs. și pentru așteptările de confidențialitate ale clienților, angajaților și partenerilor.



2 Protecție

2.1 Protecția personală

2.2 Protecția dispozitivelor

2.3 Protecția datelor

2 Protecție

2.1 Protecția personală

La nivel personal

- Instalare de soluții antivirus/ antimalware;
- Folosirea parolelor complexe;
- Introducerea de autentificare multiplă (MFA/ 2FA);
- Cursuri de educație cibernetică;
- Informare continuă despre atacurile cibernetice.

La nivelul afacerii

- Implementarea protecției la nivel personal;
- Respectarea procedurilor instituționale;
- Dubla verificare a informațiilor provenite de la colegi sau din exteriorul instituției;
- Comunicare deschisă cu departamentul IT în caz de suspiciuni ale unui atac cibernetic.

2 Protecție

2.2 Protecția dispozitivelor

La nivel personal

- Scanarea și optimizarea dispozitivelor în mod regulat;
- Respectarea avertizărilor de actualizare;
- Schimbarea periodică a parolelor (pc, mobil, router, switch, dispozitive smart) ;
- Refuzarea accesului altor persoane la rețeaua dumneavoastră de internet.

La nivelul afacerii

- Respectarea indicațiilor de nivel personal;
- Separarea rețelei pe categorii de utilizatori;
- Respectarea procedurilor de lucru și a politicilor interne;
- Restricționarea utilizării dispozitivelor din afara instituției (usb, camera web, cd...);
- Restricționarea instalării de aplicații.

2 Protecție

2.3 Protecția datelor

La nivel personal

- Creați copiilor de rezervă și salvați-le pe un alt dispozitiv;
- Acordați o atenție deosebită modului în care păstrați informațiile de identificare personală (CNP, informații financiare și alte date sensibile). Acestea sunt cel mai des folosite de atacatori pentru a comite fraude, sau furt de identitate.
- Protejați-vă permanent confidențialitatea in mediul online.

La nivelul afacerii

- Aflați ce informații personale aveți în fișierele și computerele dvs.;
- Păstrați doar ceea ce aveți nevoie pentru afacerea dvs.;
- Protejați informațiile pe care le păstrați;
- Distrugeți în mod corespunzător ceea ce nu mai este necesar;
- Creați un plan de răspuns la incidentele de securitate.

3 Educație

Educația ciberntică presupune asimilarea continuă de informații, cu ajutorul cărora să putem folosi tehnologia în deplină siguranță și tot odată să ne impunem anumite reguli de bază a folosirii acesteia, pentru a nu deveni victime ale infractorilor cibernetici.

Prin educație putem afla despre pericolele mediului online, modalități combatere a acestora și cum să reacționăm atunci când suntem victima unui atac cibernetic.

Recomandarea noastră este să parcurgeți cursurile de educație cibernetică oferite gratuit prin intermediul proiectului Cyber AID (https://www.cyberaid.eu/youtube), să vă informați din surse sigure atunci cand aveți neclarități și obligatoriu să vă protejați informațiile confidențiale și dispozitivele.

Proiectul conține și programe de educație cibernetică personalizată, destinate instituțiilor și firmelor private.

4 Îmbunătățire continuă

4.1

- Este unul dintre cei mai importanți factori pe care să ne concentrăm;
- Îmbunătățirea continua este esențială pentru a fi permanent informați în legătură cu noile amenințări și modalități de atac cibernetic, pentru a le preveni;
- Îmbunătățirea abilităților și susținerea programelor de educație cibernetică sunt întotdeauna necesare;

4 Îmbunătățire continuă

4.2

- În timp ce cunoștințele în domeniul securității cibernetice și experiența din lumea reală sunt importante pentru profesioniștii cibernetici, atribute precum abilitatea de a gândi critic, adaptabilitatea și dorința de a continua învățarea sunt la fel de importante;
- Prin intermediul proiectului CYBER AID, ne-am asumat misiunea de a reduce decalajul competențelor de securitate cibernetică cu soluții care conectează învățarea continuă. Contactați-ne pentru a vedea cum vă putem ajuta să vă îmbunătățiți postura cibernetică.

CYBER AID
EDUCATIE CIBERNETICA

WinTech consulting

CONSULTANȚĂ
ÎN SECURITATE CIBERNETICĂ

ProDefence
Cyber Security Services

SERVICII
SECURITATE CIBERNETICĂ

Proiect de educație cibernetică – destinat tuturor utilizatorilor de tehnologie

Cursuri pentru o pregătire de bază în combaterea atacurilor cibernetice
https://www.cyberaid.eu/youtube

Cursuri de educație cibernetică personalizate pentru domeniul specific de activitate

contact@cyberaid.eu
contact@prodefence.ro
contact@wintechconsulting.ro

CYSCOE
CLUSTERUL DE EXCELENȚĂ
ÎN SECURITATE CIBERNETICĂ

TOTUL DEPINDE DE NOI!

Material realizat de:
Oana Buzianu și Alexandru Angheluș